ICS 27.120.20

VDI/VDE-RICHTLINIEN

Juni 2017
June 2017

VEREIN
DEUTSCHER
INGENIEURE

VERBAND DER
ELEKTROTECHNIK
ELEKTRONIK
INFORMATIONSTECHNIK

Anforderungen an Serienprodukte und Kriterien für deren Einsatz in der Sicherheitsleittechnik in Kernkraftwerken

Allgemeiner Teil

Requirements of commercial grade products and criteria for their use in the instrumentation and control systems important to safety in nuclear power plants

General part

VDI/VDE 3528

Blatt 1 / Part 1

Ausg. deutsch/englisch
Issue German/English

Die deutsche Version dieser Richtlinie ist verbindlich.

The German version of this guideline shall be taken as authoritative. No guarantee can be given with respect to the English translation.

Inhalt Seite

Vorbemerkung ... 2
Einleitung ... 2
1 Anwendungsbereich ... 3
2 Normative Verweise ... 4
3 Begriffe ... 5
4 Abkürzungen ... 7
5 Vorgehensmodell ... 7
5.1 Relevante Einflussgrößen auf die Funktionszuverlässigkeit ... 7
5.2 Beschreibung von Designvarianten ... 9
5.3 Wege der Qualifizierung für die Kategorien A bis C ... 14
5.4 Äquivalenzprinzip ... 18
5.5 Aspekte zur Vorauswahl von Geräten/Gerätesystemen ... 20
6 Übersicht zu den Qualitäts- und Auslegungsmerkmalen ... 22
6.1 Qualitätsmerkmale der auszuwählenden Produkte (Geräte/Gerätesysteme) ... 22
6.2 Aspekte zur Systemauslegung ... 28
6.3 Randbedingungen für QS-Maßnahmen bei Projektierung, Inbetriebsetzung und Betrieb ... 34
Schrifttum ... 38

Contents Page

Preliminary note ... 2
Introduction ... 2
1 Scope ... 3
2 Normative references ... 4
3 Terms and definitions ... 5
4 Abbreviations ... 7
5 Procedural model ... 7
5.1 Relevant factors affecting the functional reliability ... 7
5.2 Description of design variants ... 9
5.3 Qualification methods for categories A to C ... 14
5.4 Equivalence principle ... 18
5.5 Aspects of the pre-selection of equipment/platforms ... 20
6 Overview of the quality and design features ... 22
6.1 Quality features of the products (equipment/platforms) to be selected ... 22
6.2 Aspects of system design ... 28
6.3 Constraints for QA measures in engineering, commissioning and operation ... 34
Bibliography ... 38

VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA)
Fachbereich Anwendungsfelder der Automation

VDI/VDE-Handbuch Automatisierungstechnik
VDI-Handbuch Energietechnik

Vorbemerkung

Der Inhalt dieser Richtlinie ist entstanden unter Beachtung der Vorgaben und Empfehlungen der Richtlinie VDI 1000.

Allen, die ehrenamtlich an der Erarbeitung dieser Richtlinie mitgewirkt haben, sei gedankt.

Eine Liste der aktuell verfügbaren Blätter dieser Richtlinienreihe ist im Internet abrufbar unter www.vdi.de/3528.

Einleitung

In der Sicherheitsleittechnik von kerntechnischen Anlagen dürfen nur nachgewiesen zuverlässige und für die jeweiligen Einsatzbedingungen geeignete Geräte verwendet werden. Je nach sicherheitstechnischer Bedeutung ergeben sich hierbei unterschiedliche Nachweistiefen und Qualitätsanforderungen für die einzelnen elektro- und leittechnischen Geräte.

Die bisher eingesetzten zumeist speziell nach kerntechnischen Gesichtspunkten qualifizierten Geräte müssen zunehmend durch neue Geräte ersetzt werden. Die am Markt verfügbaren Geräte sind zwar funktional mindestens gleichwertig und mit technologisch weit fortgeschritten Bauelementen wie Microcontrollern, FPGA (Field Programmable Gate Array) usw. aufgebaut, jedoch oft nicht nach kerntechnischen Gesichtspunkten qualifiziert. Hieraus ergeben sich vielfältige technische, organisatorische und ökonomische Fragestellungen hinsichtlich der Qualifizierung dieser Geräte für den Einsatz in der Kerntechnik. Aufgrund der relativ hohen Komplexität moderner Geräte und des relativ niedrigen Stückzahlbedarfs für kerntechnische Anlagen wird zusätzlich zu der etablierten Vorgehensweise, kerntechnisch spezifische Geräte zu entwickeln und zu qualifizieren, alternativ die Vorgehensweise verfolgt, den Einsatz geeigneter Serienprodukte in der Kerntechnik zu ermöglichen. Dies kann beispielsweise durch die Feststellung der Eignung bei Vorliegen adäquater Prüfzeugnisse aus anderen technischen Bereichen erfolgen, wobei noch zusätzliche Prüfungen zur Ergänzung der Qualifikation erforderlich sein können. Ebenso können Architekturen zum Einsatz kommen, die einen höheren Grad der Fehlertoleranz aufweisen.

Preliminary note

The content of this standard has been developed in strict accordance with the requirements and recommendations of the standard VDI 1000.

We wish to express our gratitude to all honorary contributors to this standard.

A catalogue of all available parts of this series of standards can be accessed on the Internet at www.vdi.de/3528.

Introduction

The equipment used in the instrumentation and control systems (I&C systems) important to safety deployed in nuclear facilities must be demonstrated as being reliable as well as suitable for the conditions of use in each case. There are different depths of analysis and quality requirements for the individual electrical and I&C systems depending on their importance to safety.

The devices used up to now, most of which are specially qualified in accordance with nuclear codes and standards must increasingly be replaced by new equipment. The equipment available on the market are at least functionally equivalent and consist of technologically sophisticated components such as microcontrollers, FPGA (Field Programmable Gate Arrays), etc., but they are often not qualified in accordance with nuclear codes and standards. This raises a variety of technical, organizational and economic issues with regard to the qualification of these devices for use in nuclear facilities. The relatively high complexity of state of the art equipment and the relatively low numbers of units required for nuclear facilities have prompted efforts to introduce, in addition to the established procedure of developing and qualifying devices specifically designed for use in nuclear facilities, the alternative approach of allowing to use suitable commercial grade products instead. This may for example be done by ascertaining the suitability of the latter if adequate test reports from other technical fields are available, additional tests possibly being required in order to complete the qualification. Architectures with a higher degree of fault tolerance may also be used.

Diese Richtlinie gibt Empfehlungen zu den grundsätzlichen Anforderungen, die Serienprodukte erfüllen müssen, und welche zusätzlichen Maßnahmen getroffen oder Randbedingungen geschaffen werden müssen, um diese für Funktionen der Sicherheitsleittechnik einsetzen zu können. Ziel ist es hierbei, leittechnische Systeme mit äquivalenter Zuverlässigkeit zu realisieren, und dazu auch Komponenten zu nutzen, die nach konventionellem Regelwerk qualifiziert sind, womit allerdings häufig auch zusätzliche Anforderungen an die Systemauslegung zu stellen sind.

1 Anwendungsbereich

Die Richtlinie gibt Empfehlungen zu den erforderlichen Eigenschaften von Komponenten, die in sicherheitstechnisch wichtigen elektro- und leittechnischen Einrichtungen in Kernkraftwerken eingesetzt werden sollen. Diese Eigenschaften werden hierbei im Kontext zu den leittechnischen und anlagentechnischen Randbedingungen bewertet, sodass abhängig von den vorhandenen und/ oder vorgesehenen Auslegungsmerkmalen Komponenten mit passenden Qualitätsmerkmalen zum Einsatz kommen.

Dazu werden die grundsätzlichen Anforderungen genannt, die Serienprodukte mit hochintegrierten Bauelementen und/oder mit eingebundener Software erfüllen müssen. Es wird aufgezeigt, welche zusätzlichen Maßnahmen getroffen und/oder Randbedingungen geschaffen werden müssen, um diese für Funktionen der Sicherheitsleittechnik einsetzen zu können. Ziel ist es hierbei, auch Komponenten zu nutzen, die nach konventionellem Regelwerk qualifiziert sind, um leittechnische Systeme mit äquivalenter Zuverlässigkeit zu realisieren. Hierzu sind häufig auch zusätzliche Anforderungen an die Systemauslegung zu stellen.

So können beispielsweise durch geeignete Übertragbarkeitsbetrachtungen bereits nachgewiesene Eigenschaften aus einer Qualifizierung für Sicherheitssteuerungen und Geräte nach DIN EN 61508 herangezogen werden, um diese in kerntechnischen Anlagen je nach Anwendung mit oder ohne Zusatzqualifikation einzusetzen.

In dieser Richtlinie sind die übergeordneten Anforderungen und Kriterien zum Einsatz enthalten. In den folgenden Blätter werden die Anforderungen und Kriterien für einzelne Produktgruppen abhängig von der beabsichtigten sicherheitstechnischen Funktion und Bedeutung im Anlagenkontext, dem typischen Produktaufbau und den Einsatzrandbedingungen konkretisiert.

This standard gives recommendations on the fundamental requirements which commercial grade products have to meet and on the additional measures or constraints necessary if they are to be used for the functions of I&C systems important to safety. The aim here is to implement I&C systems of equivalent reliability using also components qualified in accordance with industrial codes and standards although this means that additional requirements have to be imposed on the system's designs in many cases.

1 Scope

This standard gives recommendations on the necessary properties of components to be used in electrical and I&C systems important to safety deployed in nuclear power plants. These properties are assessed in terms of the constraints with regard to I&C and plant engineering in order to ensure that, depending on the existing and/or planned design features, components with suitable quality features are used.

For this purpose, the standard specifies the fundamental requirements which commercial grade products with high integrated components or embedded software have to meet. It shows which additional measures and/or constraints are necessary if they are to be used for the functions of I&C systems important to safety. The aim here is to also use components qualified in accordance with industrial codes and standards in order to implement I&C systems of equivalent reliability. To achieve this, it is frequently necessary to set up additional requirements on system design.

For example, suitable transferability studies allow properties already verified via a qualification for safety control systems in accordance with DIN EN 61508 to be taken as a basis for using the latter in nuclear facilities with or without an additional qualification depending on the application.

This standard contains the general requirements and criteria for use. The following parts will specify in detail the requirements and criteria for individual product groups depending on their intended safety function and their significance in the context of the plant as well as the typical product structure and the constraints for use.

Die Empfehlungen dieser Richtlinie beziehen sich auf die Errichtung oder Änderung von elektro- und leittechnischen Einrichtungen in Kernkraftwerken, deren Funktionen in die Kategorien 1 bis 3 der RSK-LL oder die Kategorien A bis C der DIN EN 61226 eingestuft sind. Die Empfehlungen dieser Richtlinie sollen als Ergänzung zu den Richtlinien zur Systemauslegung wie RSK-LL, KTA 3501, DIN EN 61513, DIN EN 60880, DIN EN 62138 angewendet werden.

Die Empfehlungen betreffen alle Komponenten, die zur Erfüllung der leittechnischen Funktionen erforderlich sind. Diese reichen vom Sensor und Messumformer über die Verarbeitungseinheiten bis zu den Schalt- und Schutzgeräten und die leittechnischen Komponenten von Antrieben (z.B. zur Rückmeldung). Die Empfehlungen dieser Richtlinie berücksichtigen damit sowohl die Errichtung oder den Austausch eines gesamten Leittechniksystems als auch den Ersatz von einzelnen peripheren Komponenten durch einen anderen Typ.

The recommendations given in this standard refer to the construction or modification of electrical and I&C systems in nuclear power plants. The functions of these systems are classified in accordance with categories 1 to 3 of RSK-LL or categories A to C of DIN EN 61226. The recommendations given in the standard are to be applied in addition to system design standards such as RSK-LL, KTA 3501, DIN EN 61513, DIN EN 60880, and DIN EN 62138.

The recommendations concern all components required in order to perform I&C functions. These range from sensors, measuring transducers and processing units to switching equipment and protective devices, and I&C components of drives (e.g. for feedback purposes). The recommendations given in the standard thus cover the construction or replacement of a complete I&C system as well as the replacement of individual peripheral components by a different type.

2 Normative Verweise / Normative references

Die folgenden zitierten Dokumente sind für die Anwendung dieser Richtlinie erforderlich: /
The following referenced documents are indispensable for the application of this standard:

DIN EN 60709*VDE 0491-7:2010-12 Kernkraftwerke; Leittechnische Systeme mit sicherheitstechnischer Bedeutung; Physikalische und elektrische Trennung (IEC 60709:2004); Deutsche Fassung EN 60709:2010 (Nuclear power plants; Instrumentation and control systems important to safety; Separation (IEC 60709: 2004); German version EN 60709: 2010)

DIN EN 60812:2006-11 Analysetechniken für die Funktionsfähigkeit von Systemen; Verfahren für die Fehlzustandsart- und -auswirkungsanalyse (FMEA) (IEC 60812:2006); Deutsche Fassung EN 60812:2006 (Analysis techniques for system reliability; Procedure for failure mode and effects analysis (FMEA) (IEC 60812: 2006); German version EN 60812: 2006)

DIN EN 60880*VDE 0491-3-2:2010-03 Kernkraftwerke; Leittechnik für Systeme mit sicherheitstechnischer Bedeutung; Softwareaspekte für rechnerbasierte Systeme zur Realisierung von Funktionen der Kategorie A (IEC 60880: 2006); Deutsche Fassung EN 60880:2009 (Nuclear power plants; Instrumentation and control systems important to safety; Software aspects for computer-based systems performing category A functions (IEC 60880:2006); German version EN 60880:2009)

DIN EN 61226*VDE 0491-1:2010-08 Kernkraftwerke; Leittechnische Systeme mit sicherheitstechnischer Bedeutung; Kategorisierung leittechnischer Funktionen (IEC 61226:2009); Deutsche Fassung EN 61226:2010 (Nuclear power plants; Instrumentation and control important to safety; Classification of instrumentation and control functions (IEC 61226:2009); German version EN 61226:2010)

DIN EN 61508*VDE 0803 Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme (IEC 61508); Deutsche Fassung EN 61508 (Functional safety of electrical/electronic/programmable electronic safety-related systems (IEC 61508); German version EN 61508)

DIN EN 61513*VDE 0491-2:2013-09 Kernkraftwerke; Leittechnik für Systeme mit sicherheitstechnischer Bedeutung; Allgemeine Systemanforderungen (IEC 61513:2011); Deutsche Fassung EN 61513:2013 (Nuclear power plants; Instrumentation and control important to safety; General requirements for systems (IEC 61513: 2011); German version EN 61513:2013)

DIN EN 62138*VDE 0491-3-3:2010-03 Kernkraftwerke; Leittechnik für Systeme mit sicherheitstechnischer Bedeutung; Softwareaspekte für rechnerbasierte Systeme zur Realisierung

von Funktionen der Kategorien B oder C (IEC 62138:2004); Deutsche Fassung EN 62138: 2009 (Nuclear power plants; Instrumentation and control important for safety; Software aspects for computer-based systems performing category B or C functions (IEC 62138:2004); German version EN 62138:2009)

DIN EN 62340*VDE 0491-10:2010-12 Kernkraftwerke; Leittechnische Systeme mit sicherheitstechnischer Bedeutung; Anforderungen zur Beherrschung von Versagen aufgrund gemeinsamer Ursache (IEC 62340:2007); Deutsche Fassung EN 62340:2010 (Nuclear power plants; Instrumentation and control systems important to safety; Requirements for coping with Common Cause Failure (CCF) (IEC 62340:2007); German version EN 62340:2010)

DIN IEC 60780:2000-12 Kernkraftwerke; Elektrisches Gerät des Sicherheitssystems; Qualifizierung (IEC 60780:1998) (Nuclear power plants; Electrical equipment of the safety system; Qualification (IEC 60780:1998))

VDI/VDE 3527:2002-07 Kriterien zur Gewährleistung der Unabhängigkeit von Sicherheitsfunktionen bei der Leittechnik-Auslegung (Design criteria serving to ensure independence of I&C safety functions)